REMARKS

Claims 1-17 are pending in the present application, of which claims 1, 8, 11, 15 and 17 are independent. No amendments have been made. Applicants believe that the present application is in condition for allowance, and respectfully request the Examiner to reconsider the rejection in light of the remarks set forth below.

I. REJECTION UNDER 35 U.S.C. §102

The Examiner rejected claims 1, 2 and 5 under 35 U.S.C. §102(e) as being allegedly anticipated by U.S. Patent No. 6,609,199 issued to DeTreville (hereinafter "DeTreville"). The rejection is respectfully traversed in its entirety.

> To anticipate a claim under 35 U.S.C. §102(e), the reference must teach every element of the claim and "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." (see MPEP §2131).

In the Office Action, the Examiner states that DeTreville teaches every element of claims 1, 2 and 5. Applicant respectfully disagrees with the characterization of DeTreville for the following reasons.

DeTreville discusses an authenticated boot methodology in which an operating system of a computer proves its identity to a microprocessor to certify that it is trusted. DeTreville teaches using the authenticated boot for the mutual authentication between an IC device 116 and a public computer that is accessible by the public (col. 4, lines 35 to 54). Particularly, it discusses equipping the CPU of the computer with a pair of public and private keys for performing the authenticated boot (col. 5, lines 54 to 65). Accordingly, in DeTreville, the public and private keys are not generated in response to a received challenge.

Upon further review of the portions cited by the Examiner, there seems to be nothing in DeTreville to even suggest generating an initial value based upon a first key from the plurality of keys generated in response to a received challenge.

For example, DeTrevillet teaches the use of a software identity register (SIR) by the CPU in executing an authenticated boot. The values of the SIR are set depending on whether a successful authenticated boot occurs (col. 6, lines 40-51 and col. 8, lines 31-42). The CPU can then generate a signed certificate containing the resultant boot log data to attest to a particular operating system (col. 9, lines 5-13). Fig. 6 shows a structure of the boot log data including the SIR or a seed field. DeTreville teaches that the CPU can use the seed to generate keys unique to the OS and processor (col. 9, lines 14-21). If this seed is considered an initial value generated based upon a key from a plurality of key and assuming for purposes of argument that the plurality of keys are generated in response to a received challenge, DeTreville does not teach or even mention concatenating the initial value with a received signal that is generated using a second key from the plurality of keys generated in response to the challenge.

Since DeTreville does not teach at least the above elements of claim 1, Applicants submit that DeTreville does not teach all elements of claim 1 and therefore, claim 1 is allowable. Also, claims 2 and 5 depend from and include all the elements cited in the independent claim 1. Accordingly, Applicant submits that these claims are believed to be allowable based on their dependency from an allowable base claim as well as other novel features included therein.

For at least the foregoing reasons, Applicants respectfully submit that DeTreville does not teach every element of the claims and request a withdrawal of the rejection under 35 U.S.C. §102.

II. REJECTION UNDER 35 U.S.C. §102

The Examiner rejected claims 8-13, 15 and 17 under 35 U.S.C. §102(e) as being allegedly anticipated by U.S. Patent No. 6,516,414 issued to Zhang et al. (hereinafter "Zhang"). The rejection is respectfully traversed in its entirety.

Zhang discusses an improved protection scheme for broadcast signals. It teaches a trusted third party that generates and passes a list of public or secret keys of receiver devices (host and POD) to a service provider (head-end system) over a secure channel. The service provider uses the list in the authentication of the respective receiver devices. Once authenticated, a receiver device may generate session keys to protect communications to the service provider (col. 4, lines 35-64). To perform authentication, the host device of the receiver device transmits its ID (H_ID) concatenated with a random number to the POD of the receiver device. The POD uses the random number to derive a counter value and sends its ID (P_ID) concatenated with H_ID to the head-end system of the service provider (col. 7, line 62 to col. 8, line 1 and col. 8, lines 33-54).

While Zhang teaches concatenation of two values, there is nothing to suggest a concatenation of a secret key with information from a mobile unit. Accordingly, Zhang does not teach or even mention generating a signature by concatenating a secret key with information from a mobile unit as in claim 8.

Similarly, while Zhang teaches generation of a plurality of keys, Zhang does not teach or even suggest generating a plurality of keys from a received value and a secret value as in claim 11. Also, in the section cited by the Examiner, Zhang mentions hashing of various values, but it does not teach generating an authorization signal from hashing a version of at least one secret key together with an authorization message.

With respect to claim 15, Zhang teaches an authentication process in which the host device sends its ID and digital signature to the POD, and the POD sends its ID and digital signature as well as the information received from the host device to the head-end system. The head-end system compares the received information to verify that the host and POD are valid devices (col. 13, lines 35-52). While Zhang mentions generation of signatures, it does not teach or suggest generating a signature by hashing a concatenated value formed from a key and a transmission message. Furthermore, Zhang does not teach or even mention generating a primary signature.

In addition, Zhang does not teach or even suggest an apparatus coupled to a mobile station, wherein the apparatus comprises a processor configured to generate a primary signature based on a key that is held private from the mobile station and a secondary signature that is received from the mobile station as in claim 17.

Since Zhang does not teach at least the above elements of the respective claims, Applicants submit that Zhang does not teach all elements of the claims and therefore, claims 8, 11, 15 and 17 are allowable. Also, claims 9-10 and 12-13 depend from and include all the elements cited in the independent claims 8 and 11 respectively. Accordingly, Applicant submits that these claims are believed to be allowable based on their dependency from an allowable base claim as well as other novel features included therein.

For at least the foregoing reasons, Applicants respectfully submit that Zhang does not teach every element of the claims and request a withdrawal of the rejection under 35 U.S.C. §102.

III. REJECTION UNDER 35 U.S.C. §103

The Examiner rejected claims 3, 4, 6 and 7 under 35 U.S.C. §103 as being unpatentable over DeTreville in view of U.S. Patent No. 6,076,162 issued to Deindl et al. (hereinafter "Deindl"). The Examiner also rejected claims 14 and 16 under 35 U.S.C. §103 as being unpatentable over Zhang in view of Applied Cryptography (hereinafter Schneier).

> To establish a prima facie case of obviousness for a claimed invention, all the claim elements must be taught or suggested by the prior art. (MPEP 2143.03)

Claims 3, 4, 6 and 7 depend from and include all the elements cited in the independent claim 1. Accordingly, Applicant submits that DeTreville does not disclose every element of claims 3, 4, 6 and 7 based on its dependency from claim 1 as well as other novel features included therein. Upon review, Deindl also does not teach the generation of a plurality of keys, the generation of an initial value and the concatenation as in independent claim 1.

Since neither DeTreville nor Deindl, separately or combined, teach or suggest all the elements, Applicants respectfully submit that the Examiner has failed to set forth a prima facie case of obviousness and respectfully requests that the rejections of claims 3, 4, 6 and 7 be withdrawn.

Similarly, claims 14 and 16 depend from and include all the elements cited in the independent claims 11 and 15, respectively. Accordingly, Applicant submits that Zhang does not disclose every element of claims 14 and 16 based on its dependency from claims 11 and 15 as well as other novel features included therein. Upon review, Deindl also does not teach the generation of a plurality of keys, the generation of a signature as in independent claims 11 and 15.

Therefore, since neither Zhang nor Deindl, separately or combined, teach or suggest all the elements, Applicants respectfully submit that the Examiner has failed to set forth a prima facie case of obviousness and respectfully requests that the rejections of claims 14 and 16 be withdrawn.

CONCLUSION

In light of the amendments contained herein, Applicants submit that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: June 7, 2005

By: Abdollah Katbab (45,325)
For. Jae-Hee Choi, Reg. No. 45,288
(858)651-5469

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502